

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

INTELLECTUAL VENTURES I LLC,
Plaintiff,

v.

SYMANTEC CORP.,

Defendant.

Case No. 10-cv-1067-LPS

JURY TRIAL DEMANDED

PLAINTIFF INTELLECTUAL VENTURES I LLC'S
RESPONSE TO
SYMANTEC'S MOTION FOR INVALIDITY UNDER 35 U.S.C. § 101

Dated: March 30, 2015

Parker C. Folse III (admitted *pro hac vice*)
Brooke A.M. Taylor (admitted *pro hac vice*)
SUSMAN GODFREY L.L.P.
1201 Third Avenue, Suite 3800
Seattle, WA 98101-3000
Telephone: (206) 516-3880
Facsimile: (206) 516-3883
pfolse@susmangodfrey.com
btaylor@susmangodfrey.com

Brian E. Farnan (Bar No. 4089)
FARNAN LLP
919 North Market Street
12th Floor
Wilmington, DE 19801
(302) 777-0300
(302) 777-0301
bfarnan@farnanlaw.com

Richard W. Hess (admitted *pro hac vice*)
Weston O'Black (admitted *pro hac vice*)
John P. Lahad (admitted *pro hac vice*)
SUSMAN GODFREY L.L.P.
1000 Louisiana Street, Suite 5100
Houston, TX 77002
Telephone: (713) 653-7859
Facsimile: (713) 654-3386
rhess@susmangodfrey.com
woblack@susmangodfrey.com
jlahad@susmangodfrey.com

Counsel for Plaintiff

Table of Contents

I.	Nature and Stage of the Proceedings	1
II.	Summary of the Argument.....	2
III.	Summary of Facts	2
IV.	Legal Standard	2
A.	Symantec Must Prove Invalidity Under § 101 by Clear and Convincing Evidence.....	2
B.	The Supreme Court’s Two-Part Test for Patent Eligibility	2
1.	<i>Mayo</i> Step One.....	3
2.	<i>Mayo</i> Step Two	5
C.	Preemption is a Fundamental Part of the Analysis	5
D.	<i>DDR Holdings</i> Provides the Most Relevant Guidance	6
V.	Argument	8
A.	The Claims of the Patents-in-Suit Are Not Directed to Abstract Ideas	8
1.	The Patents-in-Suit are Necessarily Rooted in Computer Technology	9
2.	The <i>Amici</i> Agree that the Patents-in-Suit Are Not Abstract	10
3.	The U.S. PTO Says that the Patents-in-Suit Are Not Abstract	11
4.	Symantec Mischaracterizes the Patents-in-Suit	12
a.	The ’142 Patent is Not Drawn to an Abstract Idea	13
b.	The ’050 Patent is Not Drawn to an Abstract Idea	14
c.	The ’610 Patent is Not Drawn to an Abstract Idea	16
d.	Symantec’s Cases Are Poor Analogies.....	17
B.	The Patents-in-Suit Include an “Inventive Concept”	18
1.	The Claims of the Patents-in-Suit Do Not Raise Preemption Concerns	18

a.	The '142 Patent Recites a Specific Way to Filter Email	19
b.	The '050 Patent Recites a Specific Way to Identify File Content.....	21
c.	The '610 Patent Recites a Specific Way to Perform Virus Detection	23
2.	No Software Patents Survive Symantec's Analysis.....	24
3.	Symantec Manufactures a Requirement for Patent Eligibility	25
4.	"Well-Known" Is Another Straw Man	26
5.	Symantec's Flawed Pen and Paper Argument	27
C.	The Patents-in-Suit Improve the Function of a Computer	28
D.	The Patents-in-Suit Pass the Machine-or-Transformation Test.....	29
VI.	Conclusion	30

Table of Authorities

Cases

<i>Accenture Global Servs., GmbH v. Guidewire Software, Inc.</i> , 728 F.3d 1336 (Fed. Cir. 2013).....	8, 18
<i>Alice Corp. Pty. Ltd. v. CLS Bank Int’l</i> , 134 S. Ct. 2347 (2014).....	passim
<i>Bancorp Servs., L.L.C. v. Sun Life Assurance Co. of Can.</i> , 687 F.3d 1266 (Fed. Cir. 2012).....	4
<i>Bilski v. Kappos</i> , 130 S.Ct. 3218 (2010).....	3, 25
<i>buySAFE Inc. v. Google, Inc.</i> , 765 F.3d 1350 (Fed. Cir. 2014).....	4
<i>California Institute of Tech. v. Hughes Commc’ns Inc.</i> , 2014 WL 5661290 (C.D. Cal. Nov. 3, 2014).....	passim
<i>Comcast IP Holdings I, LLC v. Sprint Commc’ns Co., L.P.</i> , 2014 WL 3542055 (D. Del. July 16, 2014)	2
<i>Content Extraction and Transmission LLC v. Wells Fargo Bank</i> , 776 F.3d 1343 (Fed. Cir. 2014).....	17
<i>Cyberfone Systems, LLC v. CNN Interactive Group, Inc.</i> , 558 Fed. App’x 988 (Fed. Cir. 2014).....	18
<i>CyberSource Corp. v. Retail Decisions, Inc.</i> , 654 F.3d 1366 (Fed. Cir. 2011).....	17
<i>DDR Holdings, LLC v. Hotels.com</i> , 773 F.3d 1245 (Fed. Cir. 2014).....	passim
<i>Dealertrack, Inc. v. Huber</i> , 674 F.3d 1315 (Fed. Cir. 2012).....	18
<i>Diamond v. Chakrabarty</i> , 100 S. Ct. 2204 (1980).....	3
<i>Diamond v. Diehr</i> , 101 S. Ct. 1048 (1981).....	4, 5, 26, 27
<i>East Coast Metal Fabricating Corp. v. Autodesk, Inc.</i> , 2015 WL 226084 (D.N.H Jan. 15, 2015).....	29

<i>Fort Properties, Inc. v. American Master Lease LLC</i> , 671 F.3d 1317 (Fed. Cir. 2012).....	4
<i>Gottschalk v. Benson</i> , 409 U.S. 63 (1972).....	4
<i>Helios Software, LLC v. SpectorSoft Corp.</i> , 2014 WL 4796111 (D. Del. Sept. 25, 2014).....	26, 30
<i>In re Bilski</i> , 454 F.3d 943 (Fed. Cir. 2008).....	29
<i>Mayo Collaborative Servs. v. Prometheus Labs., Inc.</i> , 132 S. Ct. 1289 (2012).....	passim
<i>Parker v. Flook</i> , 437 U.S. 584 (1978).....	4
<i>Planet Bingo, LLC v. VKGS LLC</i> , 576 Fed App'x 1005 (Fed. Cir. 2014).....	4
<i>SiRF Tech., Inc. v. Int'l Trade Com'n</i> , 601 F.3d 1319 (Fed. Cir. 2010).....	29, 30
<i>Smartflash LLC v. Apple, Inc.</i> , 2015 WL 661174 (E.D. Tex. Feb. 13, 2015).....	19
<i>SmartGene, Inc. v. Advanced Biological Labs., SA</i> , 555 Fed App'x 950 (Fed. Cir. 2014).....	17
<i>Synopsys, Inc. v. Mentor Graphics Corp.</i> , 2015 WL 269116 (N.D. Cal. Jan. 20, 2015).....	2
<i>Tenon & Groove, LLC v. Plusgrade S.E.C.</i> , 2015 WL 1133213 (D. Del. Mar. 11, 2015)	2
<i>TQP Development, LLC v. Intuit, Inc.</i> , 2014 WL 651935 (E.D. Tex. Feb. 19, 2014)	26
<i>Ultramercial, Inc. v. Hulu, LLC</i> , 772 F.3d 709 (Fed. Cir. 2014).....	3, 25, 29
Statutes	
35 U.S.C. § 100.....	25
35 U.S.C. § 101.....	2

Other Authorities

Examples: Abstract Ideas,

U.S. Patent and Trademark Office (Jan. 27, 2015)..... 11, 12

“A claim that presents functional and palpable applications in the field of computer technology is not excluded by Section 101. ... Such inventions should be patent-eligible because they disclose concrete technological applications and fall within patent law’s traditional bailiwick of the scientific, technological, and industrial arts.”

Symantec and Trend Micro championed this view of software patent eligibility as part of BSA | The Software Alliance’s March 6, 2015 Federal Circuit *Amicus* Brief filed in *McRo, Inc. v. Bandai Namco Games America, Inc.*, Appeal No. 2015-1080. *See* Ex. 1 at 14-15. In its present motion – filed one week later – Symantec launched a broadside attack on *all* software patents, arguing that claims describing “functions that any computer can perform” do not meet § 101 standards. The Court should reject Symantec’s sweeping indictment of software patentability, especially when it comes to the Patents-in-Suit, which pass *every* test the Supreme Court and the Federal Circuit have articulated for patent eligibility.

I. Nature and Stage of the Proceedings

Intellectual Ventures filed this case on December 8, 2010 alleging infringement of U.S. Patent Nos. 6,460,050 (“the ’050 Patent”), 6,973,142 (“the ’142 Patent”), 5,987,610 (“the ’610 Patent”), and 7,506,155 (“the ’155 Patent”) (collectively, “the Patents-in-Suit”). D.I. 1.

On June 14, 2013, Symantec moved for summary judgment of invalidity of the ’050 and ’142 Patents under 35 U.S.C. §§ 102 and 103, but not under § 101. D.I. 508. On January 6, 2015, the Court adopted Intellectual Ventures’ proposal to resolve § 101 issues post-trial. D.I. 615.

At trial, Intellectual Ventures asserted claims 9, 16, and 22 of the ’050 Patent, claim 7 of the ’610 Patent, and claims 1, 7, 21, and 22 of the ’142 Patent. The jury found that Symantec infringed the claims of the ’610 and ’142 Patents, that Symantec did not meet its burden to prove by clear and convincing evidence that any of the asserted claims are invalid, and that Intellectual Ventures was entitled to \$17 million in damages for Symantec’s infringement. D.I. 676.

II. Summary of the Argument

Symantec cannot meet its burden to prove by clear and convincing evidence that the Patents-in-Suit are invalid under § 101. The Patents-in-Suit are not drawn to abstract ideas and provide solutions necessarily rooted in computer technology to problems specifically arising in the realm of computer technology. Even if they do fall into the judicial exception (they do not), the claims of the Patents-in-Suit “add enough” “meaningful limitations” to avoid monopolizing the supposed abstract idea. And, the Patents-in-Suit improve the function of a computer and thus pass the machine or transformation test, confirming they concern patent-eligible subject matter.

III. Summary of Facts

Intellectual Ventures incorporates the relevant facts into the sections below.

IV. Legal Standard

A. Symantec Must Prove Invalidity Under § 101 by Clear and Convincing Evidence

Because the Patents-in-Suit are presumed to be valid, “an alleged infringer asserting an invalidity defense pursuant to § 101 bears the burden of proving invalidity by clear and convincing evidence.” *Synopsys, Inc. v. Mentor Graphics Corp.*, 2015 WL 269116, at *3 (N.D. Cal. Jan. 20, 2015); *Comcast IP Holdings I, LLC v. Sprint Commc’ns Co., L.P.*, 2014 WL 3542055 (D. Del. July 16, 2014) (using clear and convincing burden in § 101 analysis); *Tenon & Groove, LLC v. Plusgrade S.E.C.*, 2015 WL 1133213, at *3 (D. Del. Mar. 11, 2015) (same).

B. The Supreme Court’s Two-Part Test for Patent Eligibility

Section 101 of 35 U.S.C. provides that “[w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.” “In choosing such expansive terms modified by the comprehensive ‘any,’ Congress

plainly contemplated that the patent laws would be given wide scope.” *Bilski v. Kappos*, 130 S. Ct. 3218, 3225 (2010) (quoting *Diamond v. Chakrabarty*, 100 S. Ct. 2204, 2207 (1980)).

In *Mayo Collaborative Services v. Prometheus Labs., Inc.*, 132 S. Ct. 1289 (2012) and *Alice Corp. Pty. Ltd. v. CLS Bank Int’l*, 134 S. Ct. 2347 (2014), the Supreme Court articulated a two-part analytical framework for determining whether a patent satisfies § 101. “First, we determine whether the claims at issue are directed to one of those patent-ineligible concepts. If so, we then ask, ‘what else is there in the claims before us?’” *Alice*, 134 S. Ct. at 2355.

1. Mayo Step One

The law recognizes three “fundamental principle” exceptions to subject matter eligibility requirements: laws of nature, physical phenomena, and abstract ideas. “The concepts covered by these exceptions are part of the storehouse of knowledge of all men ... free to all men and reserved exclusively to none.” *Bilski*, 130 S. Ct. at 3225.

Symantec argues that the Patents-in-Suit fall into the “abstract idea” exception. The Supreme Court and the Federal Circuit have not defined the boundaries of an abstract idea, but Supreme Court and Federal Circuit precedent demonstrate that the vast majority of patents found to be drawn to “abstract ideas” covered long-standing fundamental economic and business practices.

In *Bilski*, for example, the Court found that the patent at issue claimed “the basic concept of hedging or protecting against risk,” which “all members of the Court agree[d]” was an abstract idea. 130 S. Ct. at 3230-31. In *Alice*, the Court held that the claims at issue “are drawn to the concept of intermediated settlement, *i.e.*, the use of a third party to mitigate settlement risk,” which like hedging, “is a fundamental economic practice long prevalent in our system of commerce.” 134 S. Ct. at 2356. In *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 715 (Fed. Cir. 2014), the Federal Circuit held that claims reciting the use of advertising as a form of currency as

applied to the Internet were drawn to an abstract idea. *See also Bancorp Servs., L.L.C. v. Sun Life Assurance Co. of Can.*, 687 F.3d 1266, 1278 (Fed. Cir. 2012) (claims implemented the abstract idea of managing a stable-value protected life insurance policy); *Fort Properties, Inc. v. American Master Lease LLC*, 671 F.3d 1317, 1322 (Fed. Cir. 2012) (finding claims involving “aggregating real property into a portfolio, dividing the interests in the portfolio into a number of deedshares, and subjecting those shares to a master agreement” disclosed an abstract investment tool); *buySAFE Inc. v. Google, Inc.*, 765 F.3d 1350, 1355 (Fed. Cir. 2014) (“the claims are squarely about creating a contractual relationship—a ‘transaction performance guaranty’—that is beyond question of ancient lineage”); *Planet Bingo, LLC v. VKGS LLC*, 576 Fed App’x 1005, 1007 (Fed. Cir. 2014) (finding claims drawn to “managing a bingo game” ineligible).

Other “abstract idea” cases generally involve attempts to patent a mathematical algorithm or formula. In *Gottschalk v. Benson*, 409 U.S. 63, 71-72 (1972), the Supreme Court found that claims involving an algorithm for converting binary-coded decimal numbers to pure binary numbers was “in practical effect ... a patent on the algorithm itself.” In *Parker v. Flook*, 437 U.S. 584, 594-595 (1978), the Court held that a mathematical formula for computing “alarm limits” in a catalytic conversion process was also an ineligible abstract idea.

The case law also provides guidance on what is *not* an abstract idea. In *Diamond v. Diehr*, 101 S. Ct. 1048, 1057-58 (1981), for example, the Supreme Court held patent-eligible a computer-implemented process for curing rubber using the Arrhenius equation, finding that the patentees “seek only to foreclose from others the use of that equation in conjunction with the all of the other steps in their claimed process.” The Supreme Court added that “when a claim containing a mathematical formula implements or applies that formula in a structure or process

which, when considered as a whole, is performing a function which the patent laws were designed to protect,” the requirements of § 101 are satisfied. *Id.* at 1060-61.

Critically, the Supreme Court cautions courts to “tread carefully in construing this exclusionary principle lest it swallow all of patent law. At some level, *all* inventions embody use, reflect, rest upon, or apply laws of nature, natural phenomena or abstract ideas.” *Alice*, 134 S. Ct. 2354 (emphasis added).

2. Mayo Step Two

If a court finds that the claims are *not* drawn to an abstract idea, the inquiry ends and the claims are eligible under § 101. Otherwise, the court applies *Mayo* step two, and “must examine the elements of the claim to determine whether it contains an ‘inventive concept’ sufficient to ‘transform’ the claimed abstract idea into a patent-eligible application.” *Alice*, 134 S. Ct. at 2357 (quoting *Mayo*, 132 S. Ct. at 1294). “A claim that recites an abstract idea must include additional features to ensure that the claim is more than a drafting effort designed to monopolize the abstract idea.” *Id.* (internal quotations omitted). In *Mayo*, the Supreme Court framed the inquiry as whether “the patent claims add *enough* to their statements” to qualify as patent-eligible processes. 132 S. Ct. at 1297.

As part of the second step, courts must disregard “well-understood, routine, conventional activity.” *Mayo*, 132 S. Ct. at 1299. A *combination* of conventional elements, however, may be unconventional, and courts must “consider the elements of each claim both individually and as an ordered combination to determine whether the additional elements transform the nature of the claim into a patent-eligible application.” *Alice*, 134 S. Ct. at 2355.

C. Preemption is a Fundamental Part of the Analysis

In *Mayo*, the Supreme Court described the principle underlying eligibility as whether a claim “forecloses more future invention than the underlying discovery could reasonably justify.”

132 S. Ct. at 1301. In *Alice*, the Supreme Court confirmed that ***preemption is “the concern that drives this exclusionary principle.”*** 134 S. Ct. at 2354.

In *California Institute of Tech. v. Hughes Communications, Inc.*, 2014 WL 5661290 at *12 (C.D. Cal. Nov. 3, 2014),¹ the court identified preemption as § 101’s main theme:

First, the concern underlying § 101 is preemption. Preemption is the idea that allowing a patent on the invention will impede innovation rather than incentivize it. This preemption concern underlies both steps of the analysis. The court must be wary about overstating this concern. By definition, every patent preempts an area of technology. A patentee with a groundbreaking invention is entitled to monopolize a segment of technology, subject to the limits of the Patent Act. Moreover, the court must be wary of litigants who exaggerate preemption concerns in order to avoid developing innovative workarounds.

This view comports with the Supreme Court’s admonition that courts “must distinguish between patents that claim the building blocks of human ingenuity and those that integrate the building blocks into something more. ... The latter pose no comparable risk of preemption, and therefore, remain eligible for the monopoly granted under our patents laws.” *Alice*, 134 S. Ct. at 2354-55. Determining patent eligibility requires analyzing the claims’ preemptive effect.

D. *DDR Holdings Provides the Most Relevant Guidance*

The Federal Circuit’s post-*Alice* opinion in *DDR Holdings, LLC v. Hotels.com*, 773 F.3d 1245 (Fed. Cir. 2014) provides helpful, relevant guidance. There, the claims involved creating web pages that permit a visitor essentially to be in two virtual places at once:

On activation of the hyperlink on a host website – such as an advertisement for a third-party merchant – instead of taking the visitor to the merchant’s website, the system generates and directs the visitor to a composite web page that displays product information from the third-party merchant, but retains the host website’s “look and feel.” Thus, the host website can display a third-party merchant’s products, but retain its visitor traffic by displaying this product information from

¹ *Cal-Tech* provides one of the most comprehensive and cohesive reviews of §101 jurisprudence to date, and nearly a dozen courts have cited the decision favorably since it issued in November 2014.

within a generated web page that “gives the viewer of the page the impression she is viewing pages served by the host” website.

773 F.3d at 1248-49. The Federal Circuit acknowledged the *Mayo/Alice* framework, *id.* at 1255, and highlighted “plainly identifiable” abstract ideas in some of its precedents (*e.g.*, *Ultramercial, buySAFE, Bancorp.*), *id.* at 1256, but also recognized that “identifying the precise nature of the abstract idea is not as straightforward as in *Alice* or some of our other recent abstract idea cases.” *Id.* at 1257.

Ultimately, the Federal Court held:

As an initial matter, it is true that the claims here are similar to the claims in the cases discussed above in the sense that the claims involve both a computer and the internet. But these claims stand apart because they do not merely recite the performance of some business practice known from the pre-Internet world along with the requirement to perform it on the Internet. ***Instead, the claimed solution is necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks.***

Id. at 1257 (emphasis added). The court found that the patent’s claims “address the problem of retaining website visitors that, if adhering to the routine, conventional functioning of the Internet hyperlink protocol, would be instantly transported away from a host’s website after ‘clicking’ on a hyperlink.” *Id.* The court also rejected the dissent’s “pre-Internet analog,” highlighting “the ephemeral nature of an Internet ‘location’” and the “near-instantaneous transport between those locations made possible by standard internet communication protocols, ***which introduces a problem that does not arise in the ‘brick and mortar’ context.***” *Id.* at 1258 (emphasis added).

The Federal Circuit also found that that “under any characterizations of the abstract idea, the ’399 patent’s claims satisfy *Mayo/Alice* step two.” *Id.* The court distinguished the claims before it from those in cases like *Ultramercial* because “the claims at issue here specify how interactions with the Internet are manipulated to yield a desired result – a result that ***overrides the***

routine and conventional sequence of events ordinarily triggered by the click of a hyperlink.”

Id. at 1258-59 (emphasis added). The court addressed preemption, saying:

It is also clear that the claims at issue do not attempt to preempt every application of the idea of increasing sales by making two web pages look the same, or of any other variant suggested by NLG. Rather, they recite a specific way to automate the creation of a composite web page by an “outsource provider” that incorporates elements from multiple sources in order to solve a problem faced by websites on the Internet. As a result, the ’399 patent’s claims include “additional features” that ensure the claims are “more than a drafting effort designed to monopolize the [abstract idea].”

Id. at 1259 (quoting *Alice*, 134 S. Ct. at 2357), and ended its § 101 analysis finding that “the claimed solution amounts to an inventive concept for resolving this particular Internet-centric problem, rendering the claims patent-eligible.” *Id.*

DDR Holdings shows that patent eligibility extends at least to (1) claims providing a solution “necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks,” (2) claims that specify interactions yielding results that “override[] the routine and conventional sequence” of Internet or computer events, and (3) claims that resolve a “particular Internet-centric problem.” *Id.* at 1258-59.

V. Argument

A. The Claims of the Patents-in-Suit Are Not Directed to Abstract Ideas

The first step is to determine “whether the claim poses any risk of preempting an abstract idea. To do so the court must first identify and define whatever fundamental concept appears wrapped up in the claim.” *Accenture Global Servs., GmbH v. Guidewire Software, Inc.*, 728 F.3d 1336, 1341 (Fed. Cir. 2013); *see also Cal-Tech*, 2014 WL 5661290 at *15 (“First, the Court must ask what these claims are trying to achieve.”).

In this case, the concepts “wrapped up” in the Patents-in-Suit—what the claims are trying to achieve—are not abstract ideas. The invention of the ’142 Patent consists of deferring delivery

of electronic mail through application of business rules and use of a quarantine. The invention of the '050 Patent consists of determining the content of a computer data file, such as whether the file contains a computer virus, using a unique digital content identifier of that computer file. The invention of the '610 Patent consists of performing computer virus detection exclusive of the networks and gateway nodes of the called and calling parties, *i.e.*, “within the telephone network.”

These claims do not cover basic tools of research and development, and do not merely recite non-patentable age-old truths, mathematical algorithms, or fundamental economic or commercial practices, such as converting binary-coded numbers to pure binary (*Benson*), calculating alarm limits (*Flook*), hedging (*Bilski*), intermediated settlement (*Alice*), managing life insurance (*Bancorp*), a real estate investment tool (*Fort*), a contractual guaranty (*buySAFE*), playing bingo (Planet Bingo), or using advertising as a form of currency (*Ultramercial*).

1. The Patents-in-Suit are Necessarily Rooted in Computer Technology

In *DDR Holdings*, the Federal Circuit distinguished the “plainly” abstract ideas in *Ultramercial*, *buySAFE*, and *Bancorp* from the case before it because the claim disclosed an invention “necessarily rooted in computer technology ... to overcome a problem specifically arising in the realm of computer networks.” 773 F.3d at 1257. The claims of the Patents-in-Suit “plainly” are **not** abstract ideas.

Like the eligible claims in *DDR Holdings*, claims of the Patents-in-Suit “do not merely recite the performance of some business practice known from the pre-Internet world along with a requirement to perform it on the Internet.” *Id.* The Patents-in-Suit have no pre-computer analog, and provide solutions “necessarily rooted in computer technology” to overcome problems specifically arising in the realm of computers and computer networks. The claims specify interactions between networked (and even non-networked) computers to, among other things,

avoid inundation with malicious or unwanted electronic mail messages, identify the content of computer files using digital identifiers, and prevent infection by malicious computer programs. These problems do not pre-date computer technology or “arise in the ‘brick and mortar’ context.” These problems have come about *because of* computer technology.

2. The Amici Agree that the Patents-in-Suit Are Not Abstract

As *amici* to the Federal Circuit, Symantec and Trend Micro agree that “*patent claims directed to a technological problem specific to the digital environment do not implement any abstract idea*” and that “when the digital environment introduces a problem that does not arise in the ‘brick and mortar’ context and the claim is directed at solving that particular problem, it typically is not an abstract idea.” Ex. 1 at 14 (citing *DDR Holdings*, emphasis added). “For the same reason,” say the *amici*, “a claim that presents functional and palpable applications in the field of computer technology is not excluded by Section 101.” *Id.*

The *amici*’s examples of “functional and palpable applications” include: (1) a software process that permits a user to quickly manipulate a digital photo by removing unwanted blemishes; (2) software that creates a means for tracking human gestures as an input mechanism for computers; and (3) user interface software that enables users to quickly and efficiently rearrange the user interface of a device. *Id.* at 15. The *amici* say “these innovations all are unique to the digital world” and “no further analysis under Section 101 is required to determine that the claim is patent-eligible.” *Id.*

Like these examples, the Patents-in-Suit solve “problems specific to the digital environment” (*i.e.*, filtering malicious and unwanted email using rules and a quarantine, computer file content identification, and computer virus detection) and satisfy Symantec’s and Trend Micro’s “functional and palpable” standard. No further analysis under § 101 is required.

3. The U.S. PTO Says that the Patents-in-Suit Are Not Abstract

The Patent and Trademark Office's recently-issued subject matter examples confirm that the claims of the Patents-in-Suit are not directed to abstract ideas. *See* Examples: Abstract Ideas, U.S. Patent and Trademark Office (Jan. 27, 2015), *available at* http://www.uspto.gov/patents/law/exam/abstract_idea_examples.pdf (Ex. 2). The PTO's first exemplary patent eligible claim involves "isolating and removing malicious code from electronic messages," and states:

A computer-implemented method for protecting a computer from an electronic communication containing malicious code, comprising executing on a processor the steps of:

receiving an electronic communication containing malicious code in a computer with a memory having a boot sector, a quarantine sector and a non-quarantine sector;

storing the communication in the quarantine sector of the memory of the computer, wherein the quarantine sector is isolated from the boot and the non-quarantine sector in the computer memory, where code in the quarantine sector is prevented from performing write actions on other memory sectors;

extracting, via file parsing, the malicious code from the electronic communication to create a sanitized electronic communication, wherein the extracting comprises

scanning the communication for an identified beginning malicious code marker,

flagging each scanned byte between the beginning marker and a successive end malicious code marker,

continuing scanning until no further beginning malicious code marker is found, and

creating a new data file by sequentially copying all non-flagged data bytes into a new file that forms a sanitized communication file;

transferring the sanitized electronic communication to the non-quarantine sector of the memory; and

deleting all data remaining in the quarantine sector.

Id. at 2. The PTO described the exemplary invention as one that "relates to software technology for isolation and extraction of malicious code contained in an electronic communication," and pronounced the claim patent-eligible because:

Such action does not describe an abstract concept, or a concept similar to those found by the courts to be abstract, such as a fundamental economic practice, a method of organizing human activity, an idea itself (standing alone), or a mathematical relationship. ***In contrast, the invention claimed here is directed towards performing isolation and eradication of computer viruses, worms, and other malicious code, a concept inextricably tied to computer technology and distinct from the types of concepts found by the courts to be abstract.***

Id. at 3 (emphasis added).

The claims of the Patents-in-Suit are similarly directed to isolation and eradication of computer viruses and malicious code and describe inventions “inextricably tied to computer technology and distinct from the types of concepts found by the courts to be abstract.”

- The ’142 Patent contemplates identifying potentially malicious or unwanted emails using business rules and transferring them to quarantine for administrator review – an invention strikingly similar to the exemplary claim that the PTO says is patent-eligible.
- The claims of the ’050 Patent are directed to characterizing or describing the content of computer files and emails, such as whether they include computer viruses. Like scanning for “malicious code markers” in the PTO’s exemplary claim, the ’050 Patent uses unique digital file content identifiers, *i.e.* hashes, to identify and characterize files.
- The computer virus detection method described in the ’610 Patent relies on determining within in the telephone network whether a piece of computer data contains a virus, and if so, inhibiting all or a portion of the computer data. This is quintessentially “technology for isolation and extraction of malicious code contained in an electronic communication.”

These concepts are clearly distinct from “a fundamental economic practice, a method of organizing human activity, an idea itself (standing alone), or a mathematical relationship” and are not “the types of concepts found by the courts to be abstract.” *Id.*

4. Symantec Mischaracterizes the Patents-in-Suit

Symantec deconstructs each Patent-in-Suit until it bears no semblance to its fundamental concept or purpose, much less the actual invention defined by the claims.

a. The '142 Patent is Not Drawn to an Abstract Idea

Symantec argues that the '142 Patent is directed to “controlling the distribution of messages based upon their content or intended recipient.” Motion at 6. Symantec tries to blur the line between “messages” and “*electronic mail* messages” (the only type of “message” the '142 Patent contemplates) by arguing that the invention “consists of applying known methods of reviewing and routing paper documents within a company to email communications.” *Id.*

The specification proves that email is different and presents problems not found in “paper documents.”

The fundamental operating paradigm of conventional post offices and mail servers is unabated delivery, which is intended to deliver an e-mail message from its sender to its recipients as directly as possible, with no interference from other users or administrators. ***

Conventionally, however, organizations have not had the ability to define and automatically enforce communication policies with respect to the handling of e-mail messages by post offices. This is because conventional post offices are designed to implement existing e-mail protocols, which are based on unabated delivery. As a result these post offices are not designed to apply business rules to e-mail messages which either intentionally delay or prohibit delivery of e-mail messages. Delayed, intercepted, or prohibited delivery is antithetical to the unabated delivery concept, and thus, conventional post offices do not provide this ability.

'142 Patent (PX2) at 1:57-63; 2:15-25. To address this “problem specifically arising in the realm of computer networks,” *DDR Holdings*, 773 F.3d at 1257, the inventors devised a solution to override the “fundamental operating paradigm,” which would “deliver an e-mail message from its sender to its recipients as directly as possible, with no interference from other users or administrators.” Instead of unabated email delivery, the '142 Patent (unconventionally) defers delivery of email through application of business rules and use of a quarantine. Symantec's italicized citations at page 7 of its Motion demonstrate that unlike hedging, intermediated

settlement, using a clearinghouse, or managing a bingo game, the inventors' solution is "necessarily rooted in computer technology."

At pages 10-11 of its Motion, Symantec tries to prove that the claims recite "long-known, conventional idea[s] performed by humans" by using a three-column table. Putting aside the glaring difference between a physical mail room and an email server, the table is hardly illuminating because it does not account for several claim elements. For example, reviewing the letter two days after receiving it is not "automatically reviewing the email message....," especially under the Court's construction, which requires "computer determination of an action..." D.I. 425 at 20. Likewise, the notion that the foreperson who filed the letter away needs to be reminded to address it is not the "*automatic review*" contemplated by the invention.

Symantec's other analogy misfires. The '142 Patent cannot plausibly be interpreted as censorship by the Post Office during World War II *done on a computer*. The claims of the '142 Patent make no sense at all if applied to snail mail.² The snail mail version would involve having the letter carrier (or someone else) review each piece of mail, deliver certain pieces, and then send certain pieces to someone else for review along with a list of which rules were triggered by the piece of mail, and then have something happen to that piece of mail if that person has not acted on it after a specified duration of time. This illogical practice is not cost-effective, exposes personal mail to potentially unwanted review, makes snail mail even slower, and underscores the glaring differences between "brick-and-mortar" and "computer" problems.

b. The '050 Patent is Not Drawn to an Abstract Idea

Symantec erroneously argues at 18 that the invention of the '050 Patent consists of "using a number to uniquely identify something and determining whether the thing has a characteristic

² The invention also does not make sense when applied to manually printing out and reviewing emails, which is outside the scope of the claims and outside the realm of computers.

based on the number.” Here, too, Symantec purposefully ignores claim elements, and collapses the invention into an overbroad idea.³ The name of the ’050 Patent is “Distributed Content Identification System,” and it is concerned with identifying the content of a computer data file or email message using a unique digital identifier – not identifying some indiscriminate thing.

As in *DDR Holdings*, the ’050 Patent does *not* “generically claim ‘use of the Internet’ to perform an abstract business practice” and *does* provide solutions necessarily rooted in computer technology to problems specifically arising in the realm of computer networks. *DDR Holdings*, 773 F.3d at 1258-59. No analog to the ’050 claims exists absent computers.

The ’050 Patent highlights “certain downsides” of the Internet:

One such downside, associated with the growth of e-mail in particular, is generally referred to as “spam” e-mail. Spam e-mail is unsolicited e-mail which is usually sent out in large volumes over a short period of time with the intent of inducing the recipient into availing themselves of sales opportunities or “get rich quick” schemes.

PX1 at 1:15-20; *see also id.* at 1:65-67 (“Another downside to the proliferation of the Internet is that it is a very efficient mechanism for delivering computer viruses to a great number of people.”). The specification also identifies another computer-specific problem: “forwarding the entire e-mail including attachments to an outside service represents a high bandwidth issue....” *Id.* at 1:50-52. These problems have no pre-computer or “brick-and-mortar” equivalents, and the claims do not “recite the performance of some business practice known from the pre-Internet world ... with the requirement to perform it on the Internet.” *DDR Holdings*, 773 F.3d at 1257.

³ As *amici*, Symantec and Trend Micro criticize the *McRo* district court for taking the same approach. According to Symantec and Trend Micro, “that approach would allow any process or method claim to be categorized as an ‘abstract idea’ because every process or method is—at bottom—the ‘idea’ of performing a series of steps to achieve a particular outcome. If section 101 excluded all such ‘ideas,’ any process claim could be rendered non-patentable.” Ex. 1 at 17 (citing *Mayo*, 132 S. Ct. at 1293).

The '050 Patent is not identifying stolen cars *on a computer*. Symantec's automobile license plate analogy is off-track. Symantec equates receiving a license plate number from a patrol officer to the "receiving..." step. Symantec does not account for the fact that the identifier must be a *digital* identifier and ignores that the '050 Patent is concerned exclusively with computer files, which can "stall" or "crash" a user's machine or a company's infrastructure, but do not curb joyriding in a stolen car. Symantec also overlooks that the digital content identifier is generated by "a file content identifier generator agent" using a computerized implementation of a mathematical algorithm – the car doesn't hammer out its own license plate.

c. The '610 Patent is Not Drawn to an Abstract Idea

Symantec argues that the '610 Patent is directed to "screening data at a location other than the location of either the sender or the intended recipient." Motion at 25. Symantec concedes, however, that this "screening" is detection of computer viruses. *Id. Computer viruses did not exist before computers*, and Symantec cannot legitimately dispute that computer viruses are "a problem specifically arising in the realm of computer networks" and computers.

The specification of the '610 Patent identifies the exclusively-digital problem:

Many computer users have virus screening and detection software installed on their computers.... Subsequent revisions of virus screening software are created and released as additional computer viruses are discovered. Consequently, each computer user has to repeatedly upgrade the virus screening software installed on his/her computer to ensure protection from recently-discovered viruses.

PX3 at 1:10-11, 1:20-23, and the necessarily-rooted-in-computer-technology solution:

Embodiments of the present invention advantageously screen computer data for viruses within a telephone network before communicating the computer data to an end user. As a result, end users can download computer data via the telephone network without concern of receiving various predetermined computer viruses.

Id. at 1:58-64.

There is no pre-computer equivalent for detecting a computer virus (let alone computer virus detection “within the telephone network”). Contrary to Symantec’s argument at 25, detecting computer viruses is not a longstanding business practice like hedging or escrow.

Symantec’s recycled World War II post office interception analogy is, again, a bridge too far, and has nothing to do with computer viruses. To even use it, Symantec must exclude computer virus screening from the concept and purpose of the claims and replace it with “reviewing data for potential *issues*,” which is much broader (and different) than the invention claimed in the ’610 Patent.

d. Symantec’s Cases Are Poor Analogies

Symantec does not address *DDR Holdings* or try to distinguish it. Instead, Symantec tries to wedge the Patents-in-Suit into factually and legally distinct cases.

In *Content Extraction and Transmission LLC v. Wells Fargo Bank*, 776 F.3d 1343, 1345 (Fed. Cir. 2014), the representative claim disclosed “receiving output representing a diversity of types of hard copy documents from an automated digitizing unit,” storing that information, “recognizing portions of said hard copy documents,” and storing that information. The Federal Circuit found that the claim was drawn to “the basic concept of data recognition and storage.” *Id.* at 1347. This is merely filing documents *on a computer*, and not a solution “necessarily rooted in computer technology” that solves problems from the computer realm like the Patents-in-Suit.

In *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1373 (Fed. Cir. 2011), the Federal Circuit reviewed a claim involving verifying credit card transactions and found the claim invalid because it was “so broadly worded that it encompassed literally *any* method for detecting fraud based on the gathered transaction and Internet data” including “logical reasoning that can be performed entirely in the human mind.” (Emphasis in original). The court found the claims in *SmartGene, Inc. v. Advanced Biological Labs., SA*, 555 Fed App’x 950, 954-55 (Fed. Cir. 2014)

invalid for the same reason. Here, the claims are not so broadly worded as to encompass any method of email filtering, file content identification, or computer virus detection, and cannot be performed entirely in the human mind. *See infra* Part V.B.5.⁴

B. The Patents-in-Suit Include an “Inventive Concept”

Because the Patents-in-Suit are not directed to an abstract idea, they are patent eligible under § 101, and the Court need not proceed to *Mayo* step two. But even assuming the Patents-in-Suit invoke supposed abstract ideas, the claims include something else – an “inventive concept” – that ensures that they do not preempt more than they should. *Mayo*, 132 S. Ct. at 1294.

1. The Claims of the Patents-in-Suit Do Not Raise Preemption Concerns

In *DDR Holdings*, the Federal Circuit found that the claims at issue “do not attempt to preempt every application of the idea of increasing sales by making two web pages look the same Rather, they recite *a specific way* to automate the creation of a composite web page by an ‘outsource provider’ that incorporates elements from multiple sources in order to solve a problem faced by websites on the Internet.” 773 F.3d at 1259 (emphasis added). Accordingly, the court held that “the claimed solution amounts to an inventive concept for resolving this particular Internet-centric problem, rendering the claims patent-eligible.” *Id.*

In *Cal-Tech*, the court concluded that meaningful limitations in the claims rendered the claims eligible:

⁴ Symantec’s remaining cases are equally distinguishable. In *Accenture Global*, the claims involved the truly longstanding business practice of processing insurance claims. 728 F.3d at 1341. In *Dealertrack, Inc. v. Huber*, 674 F.3d 1315, 1333 (Fed. Cir. 2012), the court found that the claim at issue “explains the basic concept of processing information through a clearinghouse, just as claim 1 in *Bilski II* explained the basic concept of hedging.” Identification of malicious computer files is to a clearinghouse as the iPhone is to the wheel. In *Cyberfone Systems, LLC v. CNN Interactive Group, Inc.*, 558 Fed. App’x 988 (Fed. Cir. 2014), the court affirmed the district court’s finding that the claims were “nothing more than a disembodied concept of data sorting and storage.” The Patents-in-Suit involve significantly more.

Although many of these limitations are mathematical algorithms, these algorithms are narrowly defined, and they are tied to a specific error correction process. ***These limitations are not necessary or obvious tools for achieving error correction, and they ensure that the claims do not preempt the field of error correction.*** The continuing eligibility of this patent will not preclude the use of other effective error correction techniques.

2014 WL 5661290 at *15. The court found that the claimed formula “sets forth unconventional steps for achieving error correction” and that “either individually or in combination with the claim’s other elements (including the scrambling of bits), these unconventional steps sufficiently limit preemption concerns.” *Id.* at *17-*18; *see also Smartflash LLC v. Apple, Inc.*, 2015 WL 661174, at *8 (E.D. Tex. Feb. 13, 2015) (claims eligible because they “do not risk preempting all future innovations related to exchanging access to data for payment on the Internet”).

Like the claims in *DDR Holdings*, *Cal-Tech*, and *Smartflash*, the claims here include the “meaningful limitations,” *i.e.*, the “inventive concept,” that the case law requires, and do not preempt the entire field of email filtering, file content identification, or computer virus screening.

a. The '142 Patent Recites a Specific Way to Filter Email

The '142 Patent does not preempt every application of filtering email. To the contrary, taken as an ordered combination of elements, the claims recite “a specific way” to filter email, and as discussed above, that specific way overrides email’s conventional “unabated delivery” paradigm. Claim 1 is representative:

A post office for receiving and redistributing e-mail messages on a computer network, the post office comprising:

a receipt mechanism that receives an e-mail message from a sender, the e-mail message having at least one specified recipient;

a database of business rules, each business rule specifying an action for controlling the delivery of an e-mail message as a function of an attribute of the e-mail message;

a rule engine coupled to receive an e-mail message from the receipt mechanism and coupled to the database to selectively apply the business rules to the e-mail message to determine from selected ones of the business rules a set of actions to be applied to the e-mail message; and

a distribution mechanism coupled to receive the set of actions from the rule engine and apply at least one action thereof to the e-mail message to control delivery of the e-mail message and which in response to the rule engine applying an action of deferring delivery of the e-mail message, the distribution engine automatically combines the e-mail message with a new distribution list specifying at least one destination post office for receiving the e-mail message for review by an administrator associated with the destination post office, and a rule history specifying the business rules that were determined to be applicable to the e-mail message by at least one rule engine, and automatically delivers the e-mail message to a first destination post office on the distribution list instead of a specified recipient of the e-mail message.

The Court construed “post office” to mean “an agent for receiving, storing, and distributing e-mail messages or data objects” and “rule engine” to mean “a mechanism that applies the business rules, in order to determine a set of actions (one or more) to be applied.” D.I. 425 at 22. The Court’s construction of the “combining” portion requires the email message to be combined with the new distribution list and a rule history “where a rule history identifies each of the business rule(s) whose antecedent condition was satisfied by the email message.” D.I. 425 at 18. These meaningful limitations, as construed by the Court, shrink the preemptive footprint of the invention, and describe a way to filter email that requires, among other things, a post office, a rule engine, and a distribution mechanism that each perform a specific function.

Symantec cites “recent court decisions” and argues at 13-14 that the ’142 Patent’s “selecting,” “combining,” and “automatically reviewing messages” are conventional because they are “functions that any computer can perform.” Symantec’s argument skips over several claim elements and ignores that the combination of the elements results in a specific solution to the problem of handling potentially malicious and unwanted email. For example, Symantec does not address or account for “*a rule engine* coupled to receive an e-mail message from the receipt

mechanism and coupled to the database to *selectively apply the business rules* to the e-mail message to determine from selected ones of the business rules a set of actions to be applied to the e-mail message.” PX2 at cl.1 (emphasis added). Symantec does not explain how a 15-line limitation-rich element yields “conventional” email filtering. Symantec’s conclusory allegations are not enough, especially in light of the Court’s preemption-mitigating constructions.

Symantec misplaces reliance on its “conventional” steps argument. Conventional steps are those that are ubiquitous or must be performed to implement an abstract idea. *Cal-Tech*, 2014 WL 5661290, at *14. For example, in *Mayo*, doctors needed to perform the claimed steps in order to apply the natural law:

Anyone who wants to make use of these laws must first administer a thiopurine drug and measure the resulting metabolite concentrations, and so the combination amounts to nothing significantly more than an instruction to apply the applicable laws when treating their patients.

132 S. Ct. at 1298. Here, unlike *Mayo*, the ’142 Patent’s claims are *not* needed to perform email filtering. Symantec’s alleged non-infringing alternative of sending the rule history in a separate transmission proves that the “distribution mechanism” element as claimed is not ubiquitous or necessary, and does not preempt more than it should. Ex. 3 (Trial Tr.) at 1377:1-14, 1517:20-1518:25. Likewise, as part of another purported non-infringing alternative, the “distribution mechanism” need not send a rule history to the destination post office in the first place.

b. The ’050 Patent Recites a Specific Way to Identify File Content

The ’050 Patent leverages the ability of computers to generate unique file content identifiers, such as hashes, that are not merely excised portions of the computer files. These hashes allow computers to identify the same files without communication of personal information, and with a high degree of “collision resistance,” meaning that each unique file will have its own hash with negligible chance that another non-identical file will have the same hash.

Creation of the file content identifiers requires specialized software or programming, as proved by the requirement of a “file content identifier generator agent” in claim 9, “digital ID generator agents” in claim 16, and “a client agent generating digital content identifiers” in claim 22.

In the second step of claims 9, 16, and 22, the file content identifiers are compared on a remote processing system or second tier computer to a database of other identifiers to determine “whether each received content identifier matches a characteristic of other identifiers” or whether the message has a characteristic. To this, claims of the ’050 Patent add returning, responsive to a query or request from a first tier, an “indication of the characteristic,” a “substance identifier,” or a piece of data to identify the existence or absence of a characteristic.

Taken as a whole, these claimed steps narrowly define a set of actions tied to a specific way of describing file content and classifying computer files. The innovative combination of a digitally-created unique file content identifier, a remotely-located database of content identifiers linked to content and characteristics, and a response describing the content or identifying a characteristic constitutes an unconventional and patentable approach for distributed file content identification and does not preempt the entire field of file content identification.

Symantec argues that the ’050 Patent’s “receiving,” “outputting,” and “determining” steps are conventional steps “inherent to computers.” Motion at 21. Here, too, Symantec disregards claim language in an effort to enlarge (unjustifiably) the claims’ preemptive footprint. Symantec pares down each step to “[present participle verb] + data,” *e.g.*, “receiving data” and “outputting data,” and declares them conventional. Motion at 21. Symantec says nothing about the “file content identifier” (hash), the claimed software necessary to create them, the “file content identifier generator agents,” and “the indication of the characteristic” present in the claim. These elements are not just “data” or “information.”

Symantec also argues at 21 that “requiring the method be implemented on two or more computers” does not “save its validity,” but the multi-tiered aspect of the claims is a critical aspect of the invention – it is called a “*Distributed Content Identification System*” – and further shortens the claims’ preemptive reach.

As with the ’142 Patent, Symantec’s evidence and arguments at trial betray its § 101 argument and prove that the ’050 Patent does not risk preempting all future inventions related to file content identification. First, while the ’050 Patent does not preempt the generation or use of hashes generally, at trial Symantec proposed an alleged non-infringing alternative to the ’050 Patent – one that uses excerpts of a file rather than a unique “file content identifier” as required by the claims. Ex. 3 at 1235:16-1237:25; 1510:11-1512:3. Second, as Symantec’s Dr. Spafford confirmed, the second tier could return information to the first tier, such as a count of the number of times a file had been seen, which would not be an “indication of the characteristic,” a “substance identifier,” or data to identify the existence or absence of a characteristic. *Id.* at 1580:25-1581:10. These alternatives, regardless of the unanswered questions about their feasibility, prove that the ’050 Patent includes unconventional limitations that ensure the claims are “more than a drafting effort designed to monopolize the abstract idea.”

c. The ’610 Patent Recites a Specific Way to Perform Virus Detection

The claims of the ’610 Patent likewise include meaningful limitations that trim the claimed invention to a specific way of screening for computer viruses within the telephone network. The claim language, as construed by the Court, fixes the location of virus screening, *i.e.*, outside the gateway nodes and networks of the calling or called parties, and does not preempt all virus detection. Virus detection could occur on the networks and gateway nodes of the called and calling parties, *i.e.*, not “within the telephone network.”

Additionally, virus detection “within the telephone network” would not be preempted if a call were not routed between the calling party and the called party or if computer data were not received within the telephone network, as required by the claim language. In short, the ’610 Patent captures only one form of virus detection, and its continued eligibility will not preclude the use of other virus detection techniques – even if they occur “within the telephone network.”

Symantec argues that the ’610 Patent’s steps are “the most basic functions of a computer.” Motion at 24. This argument highlights Symantec’s utter refusal to consider the elements “as an ordered combination” and neglects the context that the claim elements as a whole provide. For example, Symantec at 28 compares claim 7’s disclosure of “an identification code” to the “player identifier” and “control number” in *Planet Bingo*. Computer virus detection “within the telephone network” is nothing like playing bingo.

2. No Software Patents Survive Symantec’s Analysis

In their *amicus* brief, Symantec and Trend Micro agree with Intellectual Ventures that “claims that ‘recite a specific way’ of accomplishing a task,” including those that resolve particular computer and Internet-centric problems, “do not broadly preempt any asserted abstract idea, and are therefore patent-eligible.” Ex. 1 at 19 (citing *DDR Holdings*). They say that detailed claim language “strongly suggests that they amount to a practical application of an idea, rather than effectively claiming the idea itself.” *Id.* at 21. Symantec and Trend Micro also criticize the district court for “working backward from the issued claim by selectively removing elements,” and caution that this approach is “a recipe for unpredictable and inconsistent patent-eligibility decisions that are totally unrelated to the preemptive effect of the claim.” *Id.* at 20.

In its Motion filed one week later in this Court, Symantec completely abandons these preemption considerations – “*preemption*” isn’t even in its Motion – works backwards by selectively removing elements, and then labels the amputated claim element a conventional

“function[] that any computer can perform.” Symantec then compounds its error by failing to consider the claim elements “as an ordered combination.”

Symantec’s argument reduces to one where receiving, routing, transmitting, storing, combining, reviewing, delivering, or selecting any piece of computer data – regardless of how it is done or how it is used or what else is done – is a conventional step unworthy of patent protection. Under Symantec’s reasoning, no software is eligible. But software is patentable. *See* 35 U.S.C. § 100(b) (defining “process” in § 101 as “process, art or method, and includes a new use of a known process, machine, manufacture, composition of matter, or material”); *Ultramercial*, 772 F.3d at 715 (“[W]e do not purport to state that all software-based patents will necessarily be directed to an abstract idea.”); *Cal-Tech*, 2014 WL 5661290, at *7 (“[S]oftware must be eligible under § 101.”); *see also id.* (describing how the America Invents Act “contemplates the existence of software patents”); *Bilski*, 130 S. Ct. at 3221 (“Courts should not read into the patent laws limitations and conditions which the legislature has not expressed.”).

3. Symantec Manufactures a Requirement for Patent Eligibility

Symantec transforms step two into a referendum on the technology necessary for validity under § 101. Throughout its Motion, Symantec argues that the Patents-in-Suit are ineligible because they supposedly employ what Symantec calls “conventional” technology or “generic and conventional computing equipment.” *See, e.g.*, Motion at 7, 12-14, 16, 20, 22, 24, and 27-28. For example, Symantec says at 7 that the ’142 Patent “does not disclose any specific hardware, specialized programming, or algorithms that would permit a company to implement” the claim. *Id.* Under Symantec’s view, again, few software patents would pass muster.

Fortunately, Symantec’s view is not the law. Patents need not disclose unconventional technology, specific algorithms, or specialized computer components, and may be patent-eligible even if they rely on conventional technology and generic computers.

- In *Diehr*, the Supreme Court found computer-implemented process for curing rubber using the Arrhenius equation patent-eligible. 101 S. Ct. at 1057-58.
- In *DDR Holdings*, the Federal Circuit held claims using “a computer and the Internet” and “*standard Internet communication protocols*” eligible under § 101. 773 F.3d at 1258 (emphasis added).
- In *Helios Software, LLC v. SpectorSoft Corp.*, 2014 WL 4796111, at *17 (D. Del. Sept. 25, 2014), this Court found patent-eligible claims directed to “exchanging data over different internet sessions to capture the content of an ongoing Internet communication session,” performing “real-time data capture and transmission and reception,” and providing “access configurations and communications protocols that control computer network access and monitor activity.”
- In *Cal-Tech*, the court found that claims drawn to “encoding and decoding data for error correction” to be eligible. 2014 WL 5661290 at*15-18.
- In *TQP Development, LLC v. Intuit, Inc.*, 2014 WL 651935, at *3 (E.D. Tex. Feb. 19, 2014), Judge Bryson found claims involving “the use of a predetermined characteristic of the data being transmitted ... to trigger the generation of new key values used for encryption and decryption in a data communication system” to be valid under § 101.

These courts rightly focused on how the claims leverage computers and protocols and the preemptive effect of that use, and did not require specialized computers, unconventional protocols, or specific algorithms. Thus, use of “generic and conventional computing equipment” does not automatically render the claims ineligible, as Symantec suggests.

4. “Well-Known” Is Another Straw Man

Symantec repeatedly introduces notions of anticipation and obviousness into its Motion, hoping the Court will be distracted by its arguments about “well-known” algorithms and “prior art techniques” and incorporate §102 and §103 principles into the § 101 inquiry. Motion at 12, 16, 18, and 20. But as Symantec and Trend Micro admit in their *amicus* brief, anticipation and obviousness “must remain separate from the Section 101 inquiry.” Ex. 1 at 4.

In *Diehr*, the Supreme Court warned:

It is inappropriate to dissect the claims into old and new elements, and then to ignore the presence of the old elements in the analysis. This is particularly true in a process claim because *a new combination of steps in a process may be*

patentable even though all the constituents of the combination were well known and in common use before the combination was made.

101 S. Ct. at 1057-58 (emphasis added). Thus, “the ‘novelty’ of any element of steps in a process, or even of the process itself, is of ***no relevance*** in determining whether the subject matter of a claim falls within the § 101 categories of possibly patentable subject matter.” *Id.* Whether hashing (or any claim element of any patent) is found in the prior art is of no moment.

5. Symantec’s Flawed Pen and Paper Argument

Symantec cites inventor deposition testimony and argues § 101 invalidity because the claimed methods of the ’142 and ’050 Patents allegedly can be performed “by human thought alone” or “by using a pen and paper.”⁵ No, they cannot.

In *Cal-Tech*, the court summarily rejected the defendant’s argument that “calculating parity bit values involve mental steps that can be performed by a person with pencil and paper:”

The Court finds this mode of analysis unhelpful for computer inventions. Many inventions could be theorized with pencil and paper, but ***pencil and paper can rarely produce the actual effect of the invention.*** Likewise, with regard to software, a human could spend months or years writing on paper the 1s and 0s comprising a computer program and applying the same algorithms as the program. ***At the end of the effort, he would be left with a lot of paper that obviously would not produce the same result as the software.***

2014 WL 5661290 at *16 (emphasis added). The Court added that “it states the obvious to say that a pencil and paper cannot actually produce parity bits,” and a “pencil and paper analysis can mislead courts into ignoring a key fact: although a computer performs the same math as a human, a human cannot always achieve the same results as a computer.” *Id.*

As in *Cal-Tech*, Symantec’s “pen and paper” analysis is unhelpful to the Patents-in-Suit. Just as a pen and paper cannot actually produce *Cal-Tech*’s parity bits, a pen and paper cannot produce the same results as the ’142 and ’050 Patent’s claims. A pen and paper cannot actually

⁵ Symantec’s “pen-and-paper” argument does not appear to be directed at the ’610 Patent.

“receive an email message,” cannot actually “selectively apply [] business rules to the email message,” cannot actually defer delivery of the message by “automatically combining the email” with a new distribution list and rule history, and cannot actually deliver the email to “a first destination post office.” A pen and paper cannot actually create a digital “file content identifier” of a “data file” using a “mathematical algorithm,” cannot actually determine whether the content identifier matches a characteristic of other identifiers, and cannot actually provide an “indication of the characteristic” or a “substance identifier.” Ex. 4, 02/15/13 McDaniel Report, at ¶183.

C. The Patents-in-Suit Improve the Function of a Computer

In *Alice*, the Supreme Court recognized that claims that “purport to improve the functioning of the computer itself” or “effect an improvement in any other technology or technical field” may be patentable under § 101. 134 S. Ct. at 2359. Symantec and Trend Micro say it more succinctly and unequivocally in their *amicus* brief: “claims that **improve technology** are patent eligible.” Ex. 1 at 22 (bold in original).

At trial, Intellectual Ventures presented *unrebutted* testimony (using Symantec’s own documents) regarding the technological improvements provided by the Patents-in-Suit. The claimed inventions of the ’050 and ’610 patents shrink the period of time between identification of a computer virus or other malicious or unwanted file and distributing that information to users and customers, *i.e.*, the “protection gap.” The ’050 and ’610 patents also solve the so-called “volume problem” by offloading the database of file signatures from a user’s personal computer to the network, thereby reducing the burden on the user’s machine. Likewise, the ’142 Patent addresses filtering and deferring delivery of malicious, unwanted, or suspicious email messages in a manner that permits efficient review by an administrator. This, too, reduces strain on computing resources and increases performance by unclogging user’s inboxes and mail servers. A shorter protection gap and a reduced strain on computing resources (not to mention freedom

from malware infection) necessarily result in increased performance and “improve the functioning of the computer itself.” *See, e.g.*, Ex. 3 at 452:9-457:12, 460:11-461:6.

Symantec incorrectly argues that claims leveraging “generic and conventional computing equipment” cannot improve the functioning of a computer. Motion at 13. In *East Coast Metal Fabricating Corp. v. Autodesk, Inc.*, 2015 WL 226084, at *9 (D.N.H Jan. 15, 2015), the court adroitly captured what it means to improve computer function:

[T]he inventive concepts in [*Diehr*, *DDR Holdings*, and *Cal. Tech*] each involved an innovation that allowed a user of the invention to achieve a *better* result, rather than a result that was achieved more quickly due to the replacement of direct human activity with a computer. Those improved results are: (1) an increased ability to avoid overcuring and undercuring synthetic rubber products; (2) website connectivity that did not require a visitor to leave a host site in order to view the content of a third-party merchant’s site; and (3) more efficient correction of errors in transmitted digital data.

(internal citations omitted). In this case, the “better results” are not achieved by “replacement of direct human activity with a computer,” but include a shorter protection gap, reduced burden on computing resources, and deferring delivery of unwanted and potentially malicious email.

D. The Patents-in-Suit Pass the Machine-or-Transformation Test

The Federal Circuit’s so-called “machine-or-transformation” test provides a “useful clue” in determining patent eligibility. *Ulramercial*, 772 F.3d at 716. Under the machine-or-transformation test, “a claimed process can be patent-eligible under § 101 if: (1) it is tied to a particular machine or apparatus, or (2) it transforms a particular article into a different state or thing.” *Id.* The Federal Circuit has warned, however, that “the use of a specific machine or transformation of an article must impose meaningful limits on the claim’s scope to impart patent-eligibility.” *In re Bilski*, 454 F.3d 943, 961 (Fed. Cir. 2008) (en banc).

In *SiRF Tech., Inc. v. Int’l Trade Com’n*, 601 F.3d 1319, 1332 (Fed. Cir. 2010), the Federal Circuit emphasized that a machine will only “impose a meaningful limit on the scope of

a claim [when it plays] a significant part in permitting the claimed method to be performed.” The court found that the claims at issue were tied to a GPS receiver, and held that “the presence of the GPS receiver in the claims places a meaningful limit on the scope of the claims,” explaining:

We are not dealing with a situation in which there is a method that can be performed without a machine. ... [T]here is no evidence here that the calculations here can be performed entirely in the human mind. Here, as described, the use of GPS receiver is essential to the operation of the claimed methods.

Id. at 1333.

In *Helios Software*, this Court found the claims eligible under the machine-or-transformation test, and noted that the “implementation of the ’304 Patent by a computer inserts meaningful limitations by claiming exchanging data over different internet sessions to capture the content of an ongoing Internet communication session,” and “these meaningful limitations limit the scope of the claimed method to a machine.” 2014 WL 4796111 at *17. “Importantly,” this Court added, “none of these limitations could be performed by a human alone.” *Id.*

In this case, a computer (the machine) is critical for implementing the claims of the Patents-in-Suit, and “none of these limitations could be performed by a human alone.” *See supra*. Symantec refers to this as “incidental reliance” on a computer, but a human cannot generate a hash or describe the content of file or identify whether a characteristic is present or absent within a computer file without a computer. Likewise, it is impossible to detect computer viruses without a computer, and *electronic* mail filtering using a database of business rules and a quarantine necessarily requires a computer. Thus, as in *SiRF Tech*, “we are not dealing with a situation in which there is a method that can be performed without a machine.” 601 F.3d at 1333.

VI. Conclusion

The Patents-in-Suit are eligible under § 101, and Symantec’s motion should be denied.

Dated: March 30, 2015

Respectfully submitted,

FARNAN LLP

/s/ Brian E. Farnan

Brian E. Farnan (Bar No. 4089)
919 North Market Street
12th Floor
Wilmington, DE 19801
(302) 777-0300
(302) 777-0301
bfarnan@farnanlaw.com

Parker C. Folse III (admitted *pro hac vice*)
Brooke A.M. Taylor (admitted *pro hac vice*)
SUSMAN GODFREY L.L.P.
1201 Third Avenue, Suite 3800
Seattle, WA 98101-3000
Telephone: (206) 516-3880
Facsimile: (206) 516-3883
pfolse@susmangodfrey.com
btaylor@susmangodfrey.com

Richard W. Hess (admitted *pro hac vice*)
Weston O'Black (admitted *pro hac vice*)
John P. Lahad (admitted *pro hac vice*)
SUSMAN GODFREY L.L.P.
1000 Louisiana Street, Suite 5100
Houston, TX 77002
Telephone: (713) 653-7859
Facsimile: (713) 654-3386
rhess@susmangodfrey.com
woblack@susmangodfrey.com
jlahad@susmangodfrey.com

Counsel for Plaintiff